# 可変認証情報を用いる資格認証方法

## 発明の背景

### 発明の分野

本発明は、認証者が被認証者を認証するための資格認証方法に関する。可変認証情報を用いる認証方法とは、被認証者から認証者への認証依頼毎にパスワード等の認証情報を変更して、認証を行う方法である。

### 背景技術

従来、パスワード等の認証情報を用いて通信相手やユーザの資格を認証する方法は、公開鍵暗号方法を応用した認証方法と、共通鍵暗号方法を応用した認証方法の二つに大別することができる。しかし、インタネット関連の通信プロトコルなどへ認証技術を組み込む場合には、公開鍵暗号方法より格段の高速処理が可能な共通鍵系の暗号方法を応用した方法、特に、パスワード認証方法がよく用いられる。

基本的なパスワード認証の手順は以下の通りである。まず予め、被認証者（装置を含む）が認証者（サーバ等の装置を含む）にパスワードを登録する。認証時には、被認証者が認証者にパスワードを送信し、認証者は、受信したパスワードと登録されているパスワードを比較して認証を行う。

しかし、この方法には、次のような問題点がある。(a) 認証側にあるパスワードファイルの盗見によりパスワードが盗まれる。(b) 通信中、回線盗聴によってパスワードが盗まれる。(c) 被認証者は認証者に、自分の秘密情報であるパスワードを公開する必要がある。

最初の問題(a) を解決する方法として、例えば、被認証者が認証者に、パスワードに一方向性関数を用いた処理を施したデータを登録しておき、認証時に、認証者が受信したパスワードに同じ一方向性関数を用いた処理を施し、結果を比較するという方法がある。参考文献としては、A. Evans, W. Kantrowitz and E. Weiss: "A user authentication scheme not requiring secrecy in the computer," Commun. ACM, 17, 8, pp. 437-442 (1974)、及び R. Morris and K. Thompson:

"Password security: A case history," UNIX Programmer's Manual, Seventh Edition, 2B (1979)が挙げられる。

一方向性関数とは、入力の総当たり以外に、出力から入力を得る効率的な手段が存在しない関数であり、総当たりの計算量を充分大きくしておけば、無資格者が入力データを算出して被認証者になりすますことを防止できる。一般に、一方向性関数は、ＤＥＳやＦＥＡＬなどの共通鍵暗号方法によって得ることができる。共通鍵暗号方法は、共通秘密鍵を用いて入力される平文を処理して暗号文を出力として得るもので、平文と暗号文が与えられても共通秘密鍵が算出できない。特にＦＥＡＬでは、平文や共通秘密鍵の入力が１ビット変化しただけでも、その入力変化の痕跡をまったくとどめない出力を得ることができるという特徴を有している。

以上説明した通り、一方向性関数を用いた方法によって、基本的なパスワード認証方法の問題(a)は解決できる。しかし、これを回線盗聴が簡単なインタネットに適用する場合、問題(b) を解決することはできない。また、問題(c)に関しては、この基本的なパスワード認証方法は、銀行の顧客認証などには適用できても、同一レベルのユーザ同士の資格認証には適していない。

このような問題を解決する方法として、パスワード等の認証情報を可変にする資格認証方法がある。例えば、Lamport の方法（L. Lamport: "Password authentication with insecure communication," Commun. ACM, 24,11, pp. 770-772 (1981)）（S/KEY 型パスワード認証方式）、及び本願発明者が提案した動的パスワード認証方法である CINON 法(Chained One-way Data Verification Method)が知られている。後者に関連する文献としては、A. Shimizu, "A Dynamic Password Authentication Method Using a One-way Function" Systems and Computers in Japan, Vol. 22, No. 7, 1991, pp. 32-40、「資格認証方法」特公平８－２０５１号公報／特許第２０９８２６７号)、及び、その改良系である「ユーザ認証機能を有する情報送受信制御方法」（特願平８－２４０１９０号）や「可変認証情報を用いる資格認証方法」（特願平１１－２０７３２５号）がある。

Lamport の方法は、パスワードに一方向性関数を複数回適用しておいて、適用一回前のデータを次々と認証者側に示すことで、複数回の認証を可能にする方法

である。この方法では、最初に設定した最大認証回数から認証を実行する毎に１を減算し、認証回数を使い尽くした時点で、パスワードを再設定する必要がある。最大認証回数を増やすために一方向性関数の適用回数を増加させると処理量が増大する。銀行の顧客認証では最大認証回数として数１００～１０００等が用いられる。さらに、認証者側に比較して処理能力の小さい被認証者側での処理負担が大きいという問題点がある。

CINON 法は、被認証者（ユーザ）が認証者（ホスト）に対して、前回に正当性の検証を終え登録されている認証データのもとのデータ、次々回に認証に用いる認証データ、前回送信済みで次回の認証に用いる認証データの正当性検証データの３つのデータを認証フェーズ毎に送信することで、認証情報を安全に更新しながら次々と連鎖的に認証を行うことのできる方法である。このように、ＣＩＮＯＮ法では、被認証者が認証者の認証を得るためには、前回生成した２つの乱数$N_{(k-1)}$, $N_{(k)}$を使用する必要がある。そのため、ユーザが出先の端末から認証者の認証を得る場合には、ユーザはそれらの乱数を記憶した例えばＩＣカードの様な記憶媒体を携帯し、出先の端末で使用しなければならない。また、端末は、乱数を発生する機能及びＩＣカードを読み書きする機能を必要とする。一方、インタネットにおいては、テレビセットやワードプロセッサ、さらに携帯端末などにインタネット接続機能を付加したインタネット家電と呼ばれる製品が市場投入されようとしている。

このようなインタネット家電が普及してくることに伴い、認証処理を有する情報の送受信に対する需要が増大してくるものと思われるが、インタネット家電は、コストを最重視しているため、上述の乱数を発生したり、それらをＩＣカード等の記憶媒体へ読み書きする機構を有していない場合がほとんどである。また、処理プログラムの格納領域も限られるため、このような認証処理をできるだけ簡易で小さいプログラムサイズで実現することが望まれる。

この問題を解決するために、本出願の発明者が提案した「ユーザ認証機能を有する情報送受信制御方法」（特願平８－２４０１９０）におけるユーザ認証方式は、インターネット等のセキュリティが十分でないネットワーク上の被認証者と認証者間の情報送受信において、被認証者側にＩＣカード等の記憶媒体の読み書きを

行う機構を必要とせず、かつユーザ認証処理を小さいプログラムサイズで行うことができる安全な情報送受信制御方法と装置及びその方法を記録した記録媒体を提供することを目的としたもので、認証手順において、ＣＩＮＯＮ法の改良として、各種認証データの値を一度きりのものにするために被認証ユーザと認証サーバとの間で同期をとらなくてはならないパラメータとして、認証データ生成時に用いていた乱数に代えて、認証回数を用いるようにしたことを主要な特徴とする。被認証ユーザが行わなければならない処理が上記「資格認証方法」よりもややシンプルになっている。この発明においては、認証データの生成に用いる一方向性関数にＤＥＳやＦＥＡＬなどの共通鍵暗号方法を用いる。このため、安全性は用いる一方向性関数、すなわち共通鍵暗号方法の強度に依存し、乱数から認証回数に変更した影響はない。

さらに、本出願の発明者が提案した「可変認証情報を用いる資格認証方法」（特願平１１－２０７３２５）におけるユーザ認証方式は、被認証者は、認証フェーズ毎に乱数を生成し、乱数、ユーザＩＤ、パスワードを基に今回の認証データと次回の認証データを一方向性関数を用いて算出し、これをさらに排他的論理和を用いて被認証者以外は解読できないように暗号化し、これら今回認証用の排他的論理和及び次回認証用の排他的論理和を被認証者自身のユーザＩＤと合わせて認証者（サーバ等の装置を含む）に送信する。一方、認証者は、被認証者から前述の３つの情報を受信し、今回の認証データを基に一方向性関数を用いて算出した正当性確認パラメータと前回の認証フェーズにおいて登録した認証パラメータと比較し、一致したら今回の認証が成立したと判断し、次回の認証データを次回の認証パラメータとして登録する。したがって、セキュリティが十分でないネットワーク上の被認証者を認証者に認証させるための可変認証情報を用いる資格認証方法において、認証フェーズ毎に被認証者側および認証者側で実行する処理量（計算量）を極めて少なくすることができ、被認証側にも認証側にも簡易で小さいプログラムサイズで実現可能となり、しかも、通信路上の盗聴に強い安全な認証が行える。

上記４方式における認証方法は、全て可変認証情報を用いる資格認証方法である。かかる資格認証方法の重要な特徴は、インターネット等の通信路を通して被

認証者から認証者に渡される認証用データは、認証フェーズ毎に異なる（毎回異なる）ため、ある認証フェーズでそれが盗聴されたとしても、次の認証フェーズ（次回認証時）には別の認証データを被認証者から認証者に送らなければ認証されないので、盗聴した無資格者が正当な被認証者になりすますことができないという点である。

Lamport の方法には、被認証ユーザ側での処理（計算）量が非常に大きいという問題と、被認証者が、定期的にパスワードを更新する必要があるという問題があった。 CINON 法では、Lamport の方法の欠点であるパスワードの更新の必要性をなくすことができたが、被認証者および認証者における処理（計算）量が大きいという問題は依然残った。「ユーザ認証機能を有する情報送受信制御方式」におけるユーザ認証方法は、CINON 法の欠点である、被認証者における処理（計算量）を削減することができたが、被認証者と認証者の相互間の手順がやや複雑であり、認証サーバ側でユーザ対応に管理しなければならないデータが多く、実運用時には準正常系、異常系の処理手順を入念に検討しておく必要があるという問題があった。又、「可変認証情報を用いる資格認証方法」におけるユーザ認証方式は、「ユーザ認証機能を有する情報送受信制御方式」における管理データが多く，準正常系、異常系の処理手順が難しいという問題点を改善することができたが，今回の認証データと次回の認証データが独立していたため、ユーザ ID と今回の認証データが不変であればそれだけで認証が成立してしまうという問題点があった。さらに、悪意の第３者によって次回の認証データのみを改ざんされても認証は成立し改ざん後のデータが次回認証データとして処理されてしまうため、正当なユーザのその後の認証を妨害される恐れがあった。

## 発明の要旨

本発明の目的は、セキュリティが十分でないネットワーク上の被認証者を認証者に認証させるための可変認証情報を用いる資格認証方法において、認証フェーズ毎に被認証者側および認証者側で実行する処理量（計算量）を極めて少なくすることにより、被認証側にも認証側にも簡易で小さいプログラムサイズで実現可能とし、かつ、通信路上の盗聴や通信経路での情報の不正操作に強い安全な認証

を行える方法を提供することにある。

上記課題を解決するために、本発明による可変認証情報を用いる資格認証方法は、被認証者が認証者に対して、被認証者が秘密に保持しているパスワードを教えることなく、自分を認証させることのできる方法で、かつ被認証者から認証者への認証依頼の度に送付する認証情報を可変とする可変認証情報を用いる資格認証方法において、

初期登録フェーズは、被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、入力情報を算出することが計算量的に困難であるような一方向性を有する出力情報を生成する一方向性関数を用いて初回の認証データを生成する工程と、被認証者が認証者に対して、自己のユーザーＩＤと初回の認証データを送信する工程と、認証者が被認証者から受信した初回の認証データを初回認証時に用いる認証パラメータとして登録する工程を有し、

認証フェーズは、被認証者が、自己のユーザーＩＤとパスワードと乱数を基に、前記一方向性関数を用いて今回の認証データ用中間データと今回の認証データと次回の認証データと認証確認用中間パラメータを生成し、今回の認証データ用中間データに今回の認証データと認証確認用中間パラメータで排他的論理和演算を行うと共に，次回の認証データに今回の認証データで排他的論理和演算することにより、今回認証用の排他的論理和及び次回認証用の排他的論理和を生成する工程と、被認証者が認証者に対して、自己のユーザーＩＤ、今回認証用の排他的論理和及び次回認証用の排他的論理和を送信する工程と、認証者が、被認証者から受信した次回認証用の排他的論理和と前回登録された認証パラメータとの排他的論理和により次回認証用仮パラメータを生成し、次回認証用仮パラメータから前記一方向性関数を用いて認証確認用中間パラメータを生成する工程と，被認証者から受信した今回認証用の排他的論理和と前回登録された認証パラメータと生成された認証確認用中間パラメータとの排他的論理和を入力情報として、前記一方向性関数を用いて被認証者の正当性確認パラメータを生成し、この正当性確認パラメータと前回登録された認証パラメータを比較し、一致した場合は認証が成立したものとし、一致しない場合は認証が不成立と判断する工程と、認証が成立した場合は、前回登録された認証パラメータの替わりに前記の次回認証用仮パラメ

ータを次回認証用の認証パラメータとして登録する工程を有し、以上の工程を順次続けて被認証者の認証を行う。

すなわち、本発明では、被認証者（装置を含む）は、認証フェーズ毎に乱数を生成し、乱数、ユーザＩＤ、パスワードを基に今回の認証データと次回の認証データと認証確認用中間パラメータを一方向性関数を用いて算出し、これらの各データをさらに排他的論理和を用いて関連付け、かつ被認証者以外は解読できない形で暗号化し、これら今回認証用の排他的論理和及び次回認証用の排他的論理和を被認証者自身のユーザＩＤと合わせて認証者（サーバ等の装置を含む）に送信する。また、認証者は、被認証者から前述の３つの情報を受信し、これらの情報と前回の認証フェーズにおいて登録した認証パラメータを基に一方向性関数を用いて算出した正当性確認パラメータと前回の認証フェーズにおいて登録した認証パラメータと比較し、一致したら今回の認証が成立したと判断し、復元した次回の認証データを次回の認証パラメータとして登録するものである。

これにより、本発明では以下のような効果が得られる。

（１）前記の従来技術において１回の認証処理実行時に、被認証者と認証者との間で行われる認証関連情報の授受が、被認証者からみて１往復半（計３回の送受信）以上必要であったのに対して、被認証者が認証者に対して１回の送信のみで済む。

（２）従来技術では、認証者が被認証者毎に管理している認証関連データが４以上あるのに対して、本方式ではわずか１のデータのみで済む。

（３）認証フェーズ毎に被認証者側および認証者側で排他的論理和演算以外の暗号化又は複合処理が認証側で２回、被認証者側で５回と少なくなった。これにより、被認証者および認証者が実行する処理量（計算量）を極めて少なくすることができる。

（４）通信経路における不正操作によって、今回認証用の排他的論理和や次回認証用の排他的論理和が変更された場合、認証プロセスにおいてこれらの排他的論理和が相互に関連づけられ一方向性関数による複雑な演算もなされているため、認証ができなくなり、認証パラメータが変更されることがないので、より安全な認証を実現できる。

また、一方向性関数Ｅとしては、ＤＥＳ，ＦＥＡＬなどの秘密鍵暗号方式に用いる関数を用いることが好ましい。その場合、認証情報の解読が不可能となり、さらにＦＥＡＬを用いた場合は高速暗号処理が実現できる。

## 図面の簡単な説明

図１は、本発明の一実施例における資格認証方法の初期登録フェーズを説明する図である。

図２は、前記資格認証方法の初回認証フェーズを説明する図である。

図３は、前記資格認証方法のｋ回目認証フェーズを説明する図である。

図４は、前記資格認証方法を実施するためのシステムの一例のブロック図である。



## 望ましい実施態様

以下、本発明の好ましい実施例を説明するが、本発明はこれら実施例のみに限定されるものではなく、本発明を逸脱しない範囲で、様々な変更が可能である。

本発明による可変認証情報を用いる資格認証方法の説明に先だって、まず一方向性関数について説明する。一方向性関数とは、入力データのしらみ潰し以外に、出力データから入力データを逆算する有効な方法のない関数をいう。ＤＥＳ、ＦＥＡＬなどの秘密鍵暗号アルゴリズムを用いることにより、このような性質を実現できる。特に、ＦＥＡＬは、16ビットのパーソナルコンピュータ上のソフトウェアで200Kbps、LSIとして96Mbps（クロック10MHz）の暗号化処理速度を実現しているすぐれた秘密鍵暗号方式である。

秘密鍵暗号アルゴリズムをＣ＝Ｅ（$P_A$，$S_B$）で表す。Ｅは一方向性関数（秘密鍵暗号化処理関数、第２パラメータが秘密鍵）で、Ｃは暗号文、$P_A$は平文、$S_B$は秘密鍵である。$P_A$を平文、$S_B$を入力情報、Ｃを出力情報とすると、平文$P_A$と出力情報Ｃが分かっていても入力情報$S_B$を逆算できない。

続いて本発明の資格認証方法の実施例を説明する。本発明の認証方法のデータの流れを図１ないし図３に示す。図１は初期登録フェーズ、図２は初回認証フェーズ、図３はｋ回目認証フェーズのデータの流れを示す。データは上から下に又

は矢印に沿って流れる。図及び以下の説明において、一方向演算C＝E（$P_A$，$S_B$）をC←E（$P_A$，$S_B$）のように表す。また、排他的論理和演算子を＠で表す。

図４は本発明の資格認証方法を実現する機能ブロックの実施例を示す。図４において、１は認証制御機構、２は被認証制御機構、３は公開簿、４は秘密情報入力機構、５は乱数生成機構、６は一方向性情報生成機構、７は乱数記録機構、８は情報送信機構、９は情報受信機構、１０は情報記録機構、１１は情報比較機構、１２は演算機構である。本実施例では、認証者$U_A$を認証サーバ、被認証者$U_B$を被認証ユーザとし、その認証手順を示す。被認証ユーザ$U_B$は$P_A$として公開された自己のユーザＩＤ＝Ａを持ち、自分のみで秘密に管理するパスーワードＳを持つものとし、$S_B$としてパスーワードＳと乱数との排他的論理和を用いるものとする。

本実施例における認証方法は、大きく分けて、初期登録フェーズとその後の認証フェーズの２つのフェーズから成り立つ。認証フェーズは第１回目、第２回目、第３回目…と順次繰り返される。認証サーバ$U_A$の認証制御は認証制御機構１が行う。また、被認証ユーザ$U_B$の被認証制御は被認証制御機構２が行う。また、上記ユーザＩＤ：Ａは公開簿３に登録されている。

［初期登録フェーズ］

まず、初期登録フェーズについて説明する。

①被認証ユーザ$U_B$側（演算処理）

パスワードＳは、秘密情報入力機構４によって取り込まれる。自分のユーザＩＤとして$P_A$＝Ａを用いる。$N_{(0)}$を乱数生成機構５によって任意に設定し、乱数記録機構７によって記録しておく。一方向性情報生成機構６によって以下のデータを算出する。一方向性関数として秘密鍵暗号化処理関数Ｅを用いる。まず、初回の認証用中間データ　$E_{(0)}$←E（A，S＠$N_{(0)}$）を生成し、さらに、初回の認証データ　$E^2_{(0)}$←E（A，$E_{(0)}$）を生成する。

②被認証ユーザ$U_B$側（送信処理）

以上の準備をした上で、情報送信機構８によって認証サーバ$U_A$に、ユーザＩＤ：Ａ，初回の認証データ　$E^2_{(0)}$のデータを送信し、登録を依頼する。この場

合、盗聴の恐れのないセキュアルート（安全なルート）により送信する。

③認証サーバ$U_A$側（受信、登録処理）

情報受信機構９でユーザＩＤ：Ａおよび初回の（次回の）認証データ$E^2_{(0)}$を受信し、受信したデータ$E^2_{(0)}$を情報記録機構１０で初回の認証パラメータ（認証パラメータ初期値）Ｚとして記憶（登録）する。

［認証フェーズ］

次に、認証フェーズについて説明する。まず、初回（ｋ＝１）の認証手順について説明する。

①被認証ユーザ$U_B$側（演算処理）

乱数生成機構５により$N_1$を任意に設定し、乱数記録機構７に記憶させる。

次に、一方向性情報生成機構６によって、次回の認証データ用中間データ　$E_{(1)}$←E（A，S＠$N_{(1)}$）を生成し、さらに、次回の認証データ　$E^2_{(1)}$←E（A，$E_{(1)}$）を生成し、さらに、認証確認用中間パラメータ　$E^3_{(1)}$←E（A，$E^2_{(1)}$）を生成する。

次に、初期登録フェーズで乱数記録機構７に記憶させた$N_{(0)}$を使って、今回の認証データ用中間データ　$E_{(0)}$←E（A，S＠$N_{(0)}$）を生成し、さらに、今回の認証データ　$E^2_{(0)}$←E（A，$E_{(0)}$）を生成する。

次に、演算機構１２によって、今回認証用の排他的論理和　$F_{(0)}=E_{(0)}$＠$E^2_{(0)}$＠$E^3_{(1)}$を算出し、さらに、次回認証用の排他的論理和　$G_{(1)}=E^2_{(1)}$＠$E^2_{(0)}$を算出する。

②被認証ユーザ$U_B$側（送信処理）

情報送信機構８によって、認証サーバ$U_A$に対し、ユーザＩＤ：Ａ，今回認証用の排他的論理和$F_{(0)}$，および次回認証用の排他的論理和$G_{(1)}$のデータを送信する。この時、送信データは被認証者以外は解読できないように暗号化されているので、インターネットのような盗聴の恐れのあるルート（一般ルート）を用いてもよい。

③認証サーバ$U_A$側（受信、認証処理）

ユーザＩＤ：Ａ，今回認証用の排他的論理和$F_{(0)}$，次回認証用の排他的論理和

$G_{(1)}$を受信し、まず、次回認証用仮パラメータZ’を、演算機構１２にて以下の演算により生成する。

$$Z' \leftarrow G_{(1)} @ Z$$

ここで、$Z = E^2_{(0)}$は初期登録フェーズで情報記録機構１０に登録された認証パラメータである。次に、認証確認用中間パラメータWを、演算機構１２にて以下の演算により生成する。

$$W \leftarrow E\ (A,\ Z')$$

次に、正当性確認用中間パラメータXを、演算機構１２にて以下の演算により生成する。

$$X = F_{(0)} @ Z @ W$$

この排他的論理和演算処理において、$F_{(0)} = E_{(0)} @ E^2_{(0)} @ E^3_{(1)}$が正当な被認証ユーザ$U_B$から受信したものであれば、演算結果は$X = E_{(0)}$になるはずである。

次に、正当性確認パラメータYを、一方向性情報生成機構６にて以下の演算により生成する。

$$Y \leftarrow E\ (A,\ X)$$

もし、正当性確認パラメータYと初期登録フェーズで記憶（登録）された認証パラメータ$Z = E^2_{(0)}$が一致すれば、今回の認証が成立したことになり、一致しなければ認証は不成立となる。

④認証サーバ$U_A$側（登録処理）

認証が成立した場合、$Z' = E^2_{(1)}$を、次回すなわち第２回目の認証で用いる認証パラメータZとして情報記録機構１０に記憶（登録）する。認証が不成立の場合には、認証パラメータZは不変である。

一般に、第ｋ回目（ｋは正整数）の認証手順は以下の通りである。

①被認証ユーザ$U_B$側（演算処理）

乱数生成機構５により$N_{(k)}$を任意に設定し、乱数記録機構７に記憶させる。一方向性情報生成機構６によって、次回の認証データ用中間データ　$E_{(k)} \leftarrow E(A, S @ N_{(k)})$を生成し、さらに、次回の認証データ　$E^2_{(k)} \leftarrow E\ (A,\ E_{(k)})$を生成し、さらに、認証確認用中間パラメータ　$E^3_{(k)} \leftarrow E\ (A,\ E^2_{(k)})$を生成

する。

次に、前回の認証フェーズで乱数記録機構７に記憶させたN $_{(k-1)}$ を使って、今回の認証データ用中間データ　E $_{(k-1)}$ ←E（A，S＠N $_{(k-1)}$ ）を生成し、さらに、今回の認証データ　E$^{2}$ $_{(k-1)}$ ←E（A，E $_{(k-1)}$ ）を生成する。

次に、演算機構１２によって、今回認証用の排他論理和　F $_{(k-1)}$ ＝E $_{(k-1)}$ ＠E$^{2}$ $_{(k-1)}$ ＠E$^{3}$ $_{(k)}$ を算出し、さらに、次回認証用の排他論理和　Gk＝E$^{2}$ $_{(k)}$ ＠E$^{2}$ $_{(k-1)}$ を算出する。

②被認証ユーザU$_{B}$側（送信処理）

情報送信機構８によって認証サーバU$_{A}$に、ユーザＩＤ：A，今回認証用の排他論理和F $_{(k-1)}$ ，次回認証用の排他論理和G $_{(k)}$ のデータを送信する。この時、送信データは被認証者以外は解読できないように暗号化されているので、インターネットのような盗聴の恐れのあるルート（一般ルート）を用いてもよい。

③認証サーバU$_{A}$側（受信、認証処理）ユーザＩＤ：A，今回認証用の排他論理和F $_{(k-1)}$ ，次回認証用の排他論理和G $_{(k)}$ を受信し、まず、次回認証用仮パラメータZ’を、演算機構１２にて以下の演算により生成する。

$$Z' \leftarrow G_{(k)} \text{＠} Z$$

ここで、Z＝E$^{2}$ $_{(0)}$ は初期登録フェーズで情報記録機構１０に登録された認証パラメータである。次に、認証確認用中間パラメータWを、演算機構１２にて以下の演算により生成する。

$$W \leftarrow E（A，Z'）$$

次に、正当性確認用中間パラメータXを演算機構１２にて以下の演算により生成する。

$$X＝F_{(k-1)} \text{＠} Z \text{＠} W$$

この排他的論理和演算処理において、F $_{(k-1)}$ が正当な被認証ユーザU$_{B}$から受信したものであれば、演算結果はX＝E $_{(k-1)}$ になるはずである。

次に、正当性確認パラメータYを一方向性情報生成機構６にて以下の演算により生成する。

$$Y \leftarrow E（A，X）$$

もし、正当性確認パラメータYと前回の認証フェーズで登録された認証パラメ

ータＺ＝$E^{2}_{(k-1)}$が一致すれば、今回の認証が成立したことになり、一致しなければ認証は不成立となる。

④認証サーバ$U_A$側：

認証が成立した場合には、Ｚ’＝$E^{2}_{(k)}$を、ユーザＩＤ＝Ａの被認証ユーザが次回の認証で用いる新たな認証パラメータＺとして情報記録機構１０に記憶（登録）する。認証が不成立の場合には、認証パラメータＺは不変である。以上の認証フェーズをｋ＝１，２，３，…と順次続けて、被認証者のパスワードの認証を行う。

本実施例による資格認証方法の効果は、以下の通りである。

第ｋ回目の認証フェーズで、被認証ユーザ$U_B$が認証サーバ$U_A$に送信する今回認証用の排他論理和$F_{(k-1)}$および次回認証用の排他論理和$G_{(k)}$は、一方向性関数を用いて生成した$E^{2}_{(k-1)}$と$E^{3}_{(k)}$との排他的論理和演算により一種の暗号化並びに関連付けが施されているため、第３者に不正に盗聴されても$E^{2}_{(k-1)}$がわからない場合実データを解読することはできない。また通信経路での情報の不正操作によって今回認証用の排他論理和$F_{(k-1)}$を変更された場合認証が成り立たなくなることはもちろんのこと、$F_{(k-1)}$に、$G_{(k)}$から算出する$E^{3}_{(k)}$との排他的論理和演算が施されているため、次回認証用の排他論理和$G_{(k)}$を不正な値に変更されてしまった場合に$E^{3}_{(k)}$にあたる値が変わってしまうことから、$F_{(k-1)}$から正常な正当性確認用中間パラメータＸ及び正当性確認パラメータＹが算出できなくなり、認証自体が成り立たなくなることによって部分的な改ざんもできなくなっている。また、認証ができない場合はサーバの認証パラメータが不変となるため、より安全な認証を実現できるようになった。

第ｋ回目の認証フェーズで、認証サーバ$U_A$が被認証ユーザ$U_B$から受信した次回認証用の排他論理和$G_{(k)}$は、認証パラメータＺ＝$E^{2}_{(k-1)}$との排他的論理和演算により一種の暗号化が施されているが、$E^{2}_{(k-1)}$は、前回認証フェーズ（ｋ＝１の場合は初期登録フェーズ）において認証サーバ$U_A$に既に登録されているものであるため、$E^{2}_{(k-1)}$と再度排他的論理和演算することによって極めて簡単に、次回認証用パラメータＺ＝$E^{2}_{(k)}$を復号することができる。

さらに、今回認証用の排他論理和$F_{(k-1)}$は、認証パラメータＺ＝$E^{2}_{(k-1)}$並

びに認証確認用中間パラメータW＝$E^{3}_{(k)}$との排他的論理和演算により一種の暗号化が施されているが、認証確認用中間パラメータWは上記次回認証用パラメータから前記一方向性関数を用いて生成することができるため、正当性認証用中間パラメータX＝$E_{(k-1)}$を容易に復号することができる。排他的論理和演算は演算処理負荷が最もシンプルな一方向性関数の一つであり、かつ、２度演算すると元のデータを復元できるという特徴を持つ。

認証サーバ側において、被認証ユーザ毎に記憶（管理）しておかなければならないデータは、上記の認証パラメータZ＝$E^{2}_{(k-1)}$のわずか１つだけであり、認証フェーズ毎に認証サーバ内で実行しなくてはならない排他的論理和演算以外の復号処理（一方向性関数の使用）はわずか２回（正当性認証パラメータY，認証確認用中間パラメータWの生成）であり、処理負荷を極めて軽くすることができる。

被認証ユーザ側において、認証フェーズ毎に実行しなくてはならない排他的論理和演算以外の暗号化処理（一方向性関数の使用）は５回（今回の認証用中間データ$E_{(k-1)}$，今回の認証データ$E^{2}_{(k-1)}$，次回の認証用中間データ$E_{(k)}$，次回の認証データ$E^{2}_{(k)}$，認証確認用中間パラメータ　$E^{3}_{(k)}$）であり、処理負荷は十分に軽くてすむ。

被認証ユーザと認証サーバの相互間で行われる情報授受の回数は、認証フェーズ毎に、被認証ユーザから認証サーバへの送信が１回のみであるため、通信セッション（コネクション）の状態が不安定なネットワークにおいても確実に認証処理を行うことができる。

実施例２

実施例１では、第ｋ回目の認証フェーズで、被認証ユーザ$U_B$側で、乱数生成機構５により$N_{(k)}$を任意に設定し、乱数記録機構７に記憶させることになっているが、本実施例では、$N_{(k)}$に代えて、$E_{(k)}$および$E^{2}_{(k)}$を記憶しておく。これにより、認証フェーズ毎に被認証ユーザ$U_B$側で実行しなくてはならない排他的論理和演算以外の暗号化処理をわずか３回に削減することができる。

実施例３

実施例１では、第ｋ回目の認証フェーズで、被認証ユーザ$U_B$側で、乱数生成機構５により$N_{(k)}$を任意に設定し、乱数記録機構７に記憶させることになっているが、本実施例では認証サーバ側に認証回数を保存しておき，最初に被認証ユーザよりユーザＩＤを認証サーバに送信し，認証回数を返信してもらう。その認証回数を$N_{(k-1)}$そして認証回数+１を$N_{(k)}$の代わりに用いることによって、乱数記録機構７の無い構成においても処理できるようになる。なお，この場合認証サーバでは認証完了時に認証パラメータ$E^2_{(k)}$に加え，認証回数を1増加したものを保存するのみでよい。

以上の実施例では、認証サーバ$U_A$と被認証ユーザ$U_B$との間の資格認証方法について説明したが、インターネット利用者同士の資格認証にも本発明を適用できる。その他、本発明の趣旨を逸脱しない範囲で種々の変更が可能なことはいうまでもない。

以上説明したように、本発明による可変認証情報を用いる資格認証方法は、被認証側が認証側に対して送信するデータは一方向性関数を用いて算出し、これをさらに排他的論理和を用いて被認証者以外は解読できないように暗号化しているので、自分の秘密情報を相手に示すことなく、さらに使い捨てでない資格認証方式を実現できる。また、不正行為者が通信中の認証情報を自分に都合のいいものに改ざんした場合その情報では認証自体ができなくなるため，安全性はより確保された形となる。

また、実施例で示した認証手順では、認証される側の一方向性情報生成処理は、一回の認証につき３～５回で済む。これはLamportの方式の数100～1000回に比べて著しく小さい。また、ＣＩＮＯＮ法においても１回の認証処理実行時に、被認証者と認証者との間で行われる認証関連情報の授受が、被認証者からみて１往復半（計３回の送受信）必要であったのが、本発明では被認証者から認証者に対する１回の送信のみですむようになった。

さらに、従来技術において認証者が被認証者毎に管理している認証関連情報が４種類あったのに対して、本方式ではわずか１の情報のみですむようになった。

このように、本発明は、特に、認証フェーズ毎に被認証者側および認証者側で

実行する処理量（計算量）を極めて少なくすることができる。したがって、セキュリティが十分でないネットワーク上の被認証者を認証者に認証させるための認証方法として、被認証側にも認証側にも簡易で小さいプログラムサイズで実現可能な処理しかさせず、かつ、通信路上の盗聴や通信経路での情報の不正操作に強い安全な認証を行える方法を提供することができる。

本発明の可変認証情報を用いる資格認証方法は、ネットワーク、通信、コンピュータシステムにおけるあらゆる状況の資格認証に適用することができる。例えば、認証される側の処理量が少なく済むため、ICカードの認証システムに適用することができる。これを応用して、ICカード電話機などのシステムに適用できる。また、ネットワーク上の同一レベルのユーザ同士の相互認証に適用できる。データベースの情報へのアクセス資格の認証へ適用できる。さらに、利害関係の異なるユーザグループが同一のLAN上に共存しているような場合の、それぞれのグループの情報へのアクセス資格の認証への適用も可能である。この場合には、かなりの高速性が要求されるので、一方向性変換処理を実現する秘密鍵暗号はLSIを用いることが必要である。